IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

VIASAT, INC., **Plaintiff,** **vs.** **WESTERN DIGITAL CORPORATION, WESTERN DIGITAL TECHNOLOGIES, INC.,** **Defendants.**	**Case No. 6:21-cv-1230** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Viasat, Inc. ("Viasat") demands a trial by jury on all issues so triable and in its complaint against Defendants Western Digital Corporation and Western Digital Technologies, Inc. (collectively "Western Digital" or "Defendants"), alleging as follows:

INTRODUCTION

1. Flash memory has revolutionized computing, personal technology, gaming, enterprise data storage, and e-commerce. Through its widespread adoption, computer memory has shifted from a physical rotating platter storing magnetic ones and zeros to solid-state flash memory holding electric charges with no moving parts and few of the limitations that plagued prior memory technology. Electrical charges held in increasingly small transistors now store and power most of our digital lives.

2. But flash memory has limitations. One is that NAND flash – the most common form of flash memory – is notoriously error prone. As data is written and erased from its transistors, flash memory degrades in quality, *i.e.*, the likelihood increases that a controller or

microprocessor will read a stored electric charge representing a one as a zero (or vice versa). Moreover, as the transistors in flash memory become denser, as they have over time, the likelihood of errors also increases. These errors undermine flash's usefulness. Bad data can slow down devices and weaken flash's advantages over prior memory technology.

3. Given these limitations, there is substantial value in figuring out how to eliminate or fix flash errors quickly while utilizing as little power as possible. The most important tool for eliminating flash errors is having robust error-correction protocols that allow controllers or microprocessors to identify and fix errors on the fly. But these protocols can also slow devices down, and there was a need to develop an architecture that could fix errors quickly or even ensure that the errors do not happen in the first place.

4. Viasat is a global communications company, with significant expertise in engineering satellite, terrestrial wireless, and optical communications solutions. The named inventors, employees at Viasat at the time the patents at issue were filed, used the knowledge they had gained designing error-correction systems for satellites and fiber optics to design an improved architecture for error correction in flash. As information passes from transistors to a controller and on to an electronic device, flash memory functions as a communication channel – just like a satellite beaming signals down to a rooftop antenna. These engineers designed an improved way to structure flash error correction, including a novel architecture and the ability to adapt to degradation in flash memory's reliability.

5. Their work resulted in U.S. Patent Numbers 8,615,700 (the '700 patent) and 8,966,347 (the '347 patent), asserted here.

NATURE OF THE ACTION

6. This is a civil action for patent infringement under the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

7. Viasat is the owner of all rights, title, and interest in the '700 patent and the '347 patent.

8. Western Digital has infringed and is still infringing the '700 and '347 patents, directly and indirectly, by making, using, offering for sale or selling in the United States, including in this District, certain products that implement the patents' error-correction architecture. Specifically, Western Digital's NAND-flash-memory-containing products, all of which, on information and belief, include Western Digital's "proprietary Sentinel ECC&DSP technology."[1]

9. Examples of potentially infringing products include flash memory enterprise solutions for "Data-Centric Architectures" sold under the brand names Western Digital, G-Technology, SanDisk, Ultrastar, WD, Cloudspeed, iNAND, and OpenFlex (the "Accused Products").[2] Such architectures potentially include internal hard disk drives, internal solid state drives, commercial internal drives, data center drives, data center platforms, embedded flash,

[1] *See The Application of ECC/DSP to Flash Memory* at 5, available online at https://documents.westerndigital.com/content/dam/doc-library/en_us/assets/public/western-digital/collateral/white-paper/white-paper-the-application-of-ecc-dsp-to-flash-memory.pdf (last visited Sept. 15, 2021) ("Western Digital's proprietary Sentinel ECC&DSP™ technology is embedded in all its NAND controllers. It is a mature technology with 15 generations deployed within Western Digital's controllers across various product lines (enterprise and client grade SSD, embedded NAND, memory cards, USB drives, etc.).".

[2] *See Western Digital Expands Flash Portfolio for Scaling Data-Centric Architectures in the Zettabyte Era*, available online at https://www.westerndigital.com/company/newsroom/press-releases/2020/2020-11-09-western-digital-expands-flash-portfolio-for-scaling-data-centric-architectures (last visited Sept. 14, 2021).

USB flash drives, commercial removable storage, memory cards, external desktop drives, portable drives, personal cloud/NAS drives, and accessories.[3]

10. This list of Accused Products is non-limiting and based on information currently available to Viasat. Viasat reserves the right to modify the list of Accused Products, including as new products and iterations of older products are released during the pendency of this case.

11. Viasat seeks monetary damages.

THE PARTIES

12. Plaintiff Viasat is a global communications company based in San Diego, California, and organized under the laws of Delaware. Viasat's headquarters are at 6155 El Camino Real, Carlsbad, CA 92009-1699.

13. Viasat maintains an established place of business in this District at 111 Sandra Muraida Way, STE. 100, Austin, TX 78703. Viasat employs approximately 30 individuals in its Austin office in several different technical areas.

14. On information and belief, Defendant Western Digital Corporation is a Delaware corporation with its principal place of business at 5601 Great Oaks Parkway, San Jose, CA 95119. Either directly or through its subsidiaries, Western Digital Corporation also has a place of business at 7501 North Capital of Texas Highway, A-100, Austin, TX 78731.

15. On information and belief, Defendant Western Digital Technologies, Inc. is a Delaware corporation and subsidiary of Western Digital Corporation. Its principal place of business is 5601 Great Oaks Parkway, San Jose, CA 95119, but it also maintains a place of business at 7501 North Capital of Texas Highway, A-100, Austin, TX 78731.

[3] *See e.g., Products & Resources: Product Portfolio*, available online at https://www.westerndigital.com/product-portfolio (last visited Sept. 14, 2021).

16. Western Digital Technologies, Inc. is registered with the Texas Secretary of State to do business in Texas. Western Digital Technologies, Inc. has a registered agent for the service of process in Texas with Corporation Service Company, d/b/a CSC -Lawyers Incorporating Service Company, 211 East 7th Street, Suite 620, Austin, TX 78701.

17. Western Digital designs, manufactures, and sells throughout the world a wide range of flash memory products that incorporate Viasat's patented error-correction technologies.

JURISDICTION AND VENUE

18. This is a civil action for patent infringement arising under the Patent Laws of the United States, Title 35 of the United States Code.

19. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a) and 35 U.S.C. § 271 *et seq*.

20. The Court's exercise of personal jurisdiction over the Defendants complies with both the Texas long-arm statute and the Due Process Clause of the Fourteenth Amendment. The Defendants do continuous and systematic business in this District, including by providing infringing products and services to residents of this District and by soliciting business from residents in this District. The Defendants also make infringing sales in this District.

21. The Defendants have purposely directed their activities toward Texas and have purposefully availed themselves of the privileges of conducting activities in the state. Western Digital has maintained a physical presence in this District for years. Tax records show that Western Digital Technologies, Inc. has owned and maintained property at 7501 N. Capital of Texas Highway, Suite A-100, Austin, TX 78731 from at least 2016 through today. The Defendants conduct business from their property at 7501 N. Capital of Texas Highway, Suite A-

100, Austin, TX 78731. In addition, Western Digital Technologies, Inc. has owned property at 19000 Limestone Commercial Drive 500, Pflugerville, Texas 78660 since at least 2019.

22. Western Digital also employs individuals in this District who, on information and belief, contribute to the Defendants' sales of infringing products. On information and belief, Western Digital employees in this District include the Director, Global Channel and OEMs, who is the team lead for the marketing of Western Digital's SSD enterprise storage products (Scott Glenn); engineers involved in the design of firmware, microprocessor design, and high-throughput computing (Robert Golla, Srini Vimuri); and individuals responsible for the marketing and sales of infringing products (Rick Vasquez).

23. The Defendants have also sought to recruit individuals for employment within the District through its website, LinkedIn, and other websites. This includes a recent posting seeking to hire a Research Staff Member in the CPU development group.[4]

FACTUAL BACKGROUND

24. Viasat is a global communications company founded in 1986 in Carlsbad, California.[5]

25. Viasat's businesses range from providing resilient communications services to the U.S. Department of Defense and other allied militaries to offering broadband connectivity to

[4] *See* LinkedIn, Senior Technologist, R&D Engineering CPU's Job Listing, available online at https://www.linkedin.com/jobs/search/?currentJobId=2691325462&keywords=western%20digital%20austin (last visited Sept. 14, 2021).

[5] *See Viasat History, Innovation & Industry Firsts*, available online at https://www.viasat.com/about/history/ (last visited Sept. 15, 2021).

residential and commercial aviation customers around the globe.[6] Viasat currently provides high-speed internet service to nearly 1,500 commercial airliners, has over 500,000 residential broadband subscribers in the U.S., and employs over 5,800 employees in over 60 offices around the world. In fiscal year 2021, Viasat generated $2.3 billion in revenues and spent over $115 million on independent research and development, including in support of a forthcoming global satellite network expected to provide over 3 terabytes per second of data capacity from space.

26. At its core, Viasat innovates how to successfully and efficiently move large quantities of data. Viasat's engineers work to solve technical challenges relating to communications channels, with an emphasis on satellites. Satellites are essential to the world's modern communications systems. Whether downloading an app or responding to emails in-flight, Viasat satellites route information via electromagnetic signals sent between the satellites twenty-two thousand miles overhead and users on earth. Over these long distances, data must pass through the harsh conditions of outer space, not to mention clouds, storms, trees, and other obstructions, each potentially degrading the signal and causing data loss through the creation of noise and errors. Noise and errors in data transmitted across a communication system or stored and then retrieved can render the data unusable. And unusable information can frequently be the same as no information.

27. Transmitting data across a satellite channel or data storage system thus requires ways to ensure the integrity of the data that is being sent and received. One potential method for doing so would be to require retransmission of data from a given host to correct errors. But

[6] *See Viasat Space and Networking Technology*, available online at https://www.viasat.com/business-and-commercial/space-and-networking-technology/ (last visited Sept. 15, 2021).

retransmission has its limitations. It requires an entire data message to be re-sent even if only a part is corrupted, in turn clogging the channel. Even then, some errors are to be expected due to noise in any transmission or retrieval of data, leaving the same problem that retransmission seeks to fix.

28. Channel coding is the science of adding controlled redundancy to make a data message robust to noise, or errors caused by noise. In the context of satellite communication, Viasat developed novel systems for channel coding known as "forward error correction" (or FEC), which gives the *recipient* of a signal the ability to correct certain errors in the data without requiring retransmission.

29. For years, Viasat has worked to implement industry-leading FEC in its satellite systems. In 1996, Bill Thesling and Mark Vanderaar founded Efficient Channel Coding after the two met performing communications research for NASA. Efficient Channel Coding designed satellite communications components and systems for both the public and private sectors. The company – including the named inventors of the '700 and '347 patents – designed the software and hardware necessary to ensure effective satellite communications. FEC was one of the many areas where the inventors focused their energies.

30. Viasat purchased Efficient Channel Coding in 2005, after which the team broadened its focus to new and different markets in which to apply the innovations they had created for satellite communications. One of those markets was flash memory.

31. At its most fundamental, flash memory consists of electrical charges stored in transistors. These charges represent binary digits or bits. In single-level cells, an electrical charge represents a 1 and a lower charge represents a 0. Bits are the smallest unit of information in computer technology. When strung together, these bits form more complex data structures from

bytes (8 bits) to gigabytes (approximately 1,000,000,000 bytes). In turn, these strings of bits collectively represent apps, programs, documents, and countless other forms of digital information.

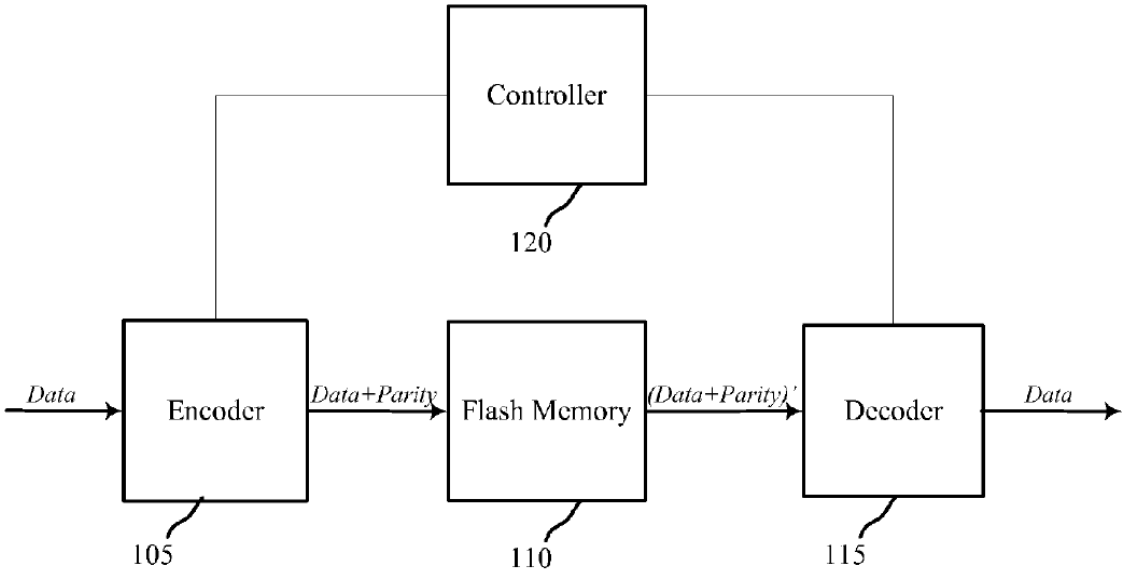
32. Flash memory is usually associated with a controller. A controller is a microprocessor that regulates how data is stored in flash memory and how it is retrieved. For example, when saving a photograph to a flash drive, the controller will send all the 1s and 0s representing that photograph to the flash memory and dictate where that data should be stored or "written" as electrical charges in the flash memory. And when a user wants to open and view the photograph, the controller determines what electrical charges should be "read" from which portions of the flash memory and will then route that data so that the image can be displayed on a screen. Unlike some other forms of memory, the charge held in a flash-memory transistor – representing a 1 or a 0 – is stored even when unpowered.

33. Reading and writing to flash memory inherently results in errors, especially as data is written or rewritten multiple times. When the '700 and '347 patents' inventors turned their attention to flash memory, it was increasingly being used in computers, enterprise storage, and consumer technology. As processing speed increased, so too did the need for greater storage capabilities. These converging trends began to pose problems with the integrity of the data being stored in and retrieved from flash memory. For example, flash memory began incorporating more and smaller transistors. As these transistors got more compact, they held less charge. This increased the probability of memory errors because of the more exact measurement needed to figure out if the charge represented a 1 or a 0. Plus, rather than store a single bit in each transistor, flash memory began holding multiple bits. This too resulted in each bit being represented by a smaller charge, compounding the difficulties in measuring the stored charge.

34. The ’700 and ’347 patents’ inventors recognized that the increasingly common errors then arising with flash memory were similar to the types of problems they had encountered when designing satellite systems. Just as it was foreseeable that a rainstorm would degrade some portion of the signal sent from a satellite, bit errors were going to occur in reading data from increasingly small electrical charges in flash memory. And because flash memory was becoming more widespread in broader applications, controllers would be processing more data even while users were expecting higher levels of both data fidelity and speed.

35. To the inventors, these were problems that demanded innovation in error correction. Although error correction systems existed for flash already, the inventors focused on how to improve those systems in light of the challenges posed by flash’s increasing use and data flow and their experience designing error-correction systems in other contexts.

36. As depicted below, FEC in flash memory is implemented in the flash controller. Data flows into an encoder that takes the information and adds redundancy that creates an error correction coding (ECC) signature for that data. This data and the ECC signature are then transmitted into a memory cell (the flash memory) and stored together there. When the controller accesses the stored data at a later point in time, it reads both the original underlying data and the associated ECC signature and a new ECC signature is formed for the retrieved data. The original and the new ECC signatures are compared. If the ECC signatures match, there is no error and the data is sent on. If they do not match, however, an error has occurred and the controller then attempts to correct the error before sending it on.



37. Some algorithms for a controller to implement error detection and correction were generally known in 2010. Nevertheless, the ’700 and ’347 patent inventors determined that error detection and correction in flash memory could be improved. The patents at issue, entitled “Forward error correction with parallel error detection for flash memories,” are the result of that work.

38. The ’700 and ’347 patents list as inventors Sameep Dave, Russell Fuerst, Mark Kohoot, Jim Keszenheimer, and William H. Thesling.

39. The ’700 patent issued on December 24, 2013.

40. The ’347 patent issued on February 24, 2015.

41. Both the ’700 and ’347 patents are assigned to Viasat, Inc.

42. Unlike previous systems, the ’700 patent claims an error-correction architecture that, among other things, parallelized error detection and physically separated error correction from error detection. And the ’347 patent claims a method for optimizing flash error correction in response as the memory ages or becomes especially error prone over time.

43. These improvements to otherwise known error-correction architectures are not abstract ideas. The ’700 patent addresses, among other things, a specific improvement to the way that electronic devices are structured to detect and correct errors in flash memory, including specific claimed materials, structures, and configurations of an error-correction system that provides enhanced error correction for flash devices. The ’347 patent addresses situations where flash memory begins to degrade. For example, as the errors from a particular section of flash meet a threshold, the claimed ’347 patent’s method provides that additional resources will be powered up to assist in error correction.

44. There are many benefits associated with the error-correction architecture claimed in the ’700 and ’347 patents. Among them, the claimed architecture provides for higher data throughput, lower power consumption, and higher data integrity. The architecture also contributes to the overall reliability and longevity of flash memory devices. And the claimed error-correction system makes it possible for the controller to dynamically manage flash memory’s operation over the life of the device.

WESTERN DIGITAL’S INFRINGING PRODUCTS

45. Western Digital manufactures and sells data-storage devices containing flash memory with ECC systems that infringe the ’700 and ’347 patent claims, including flash-based solid-state drives (SSDs) for a wide array of uses, such as enterprise storage and data centers.

46. Western Digital makes, uses, sells, offers to sell, imports, or otherwise distributes and supports the Accused Products in the United States.

47. On information and belief, Western Digital conducts research and development and testing of the Accused Products in the United States. Western Digital also manufactures Accused Products outside of the United States and sells them to third parties with the knowledge

that the Accused Products will be imported for use in the United States. All of these activities contribute to Western Digital's revenues in the United States.

48. Western Digital maintains a website through which it advertises and sells the Accused Products, including touting the infringing error-correction architecture in its SSDs.[7]

49. According to Western Digital, all of its NAND-flash-memory-containing products (like SSDs) utilize its proprietary Sentinel ECC&DSP error correcting system. The Sentinel ECC&DSP error correcting system has what Western Digital describes as a "multi-gear architecture."[8] The Sentinel ECC&DSP error correcting system monitors the bit-error rate for the flash memory and selects a higher or lower power "gear" for the error correcting system depending on the severity of the bit-error rate.[9] As shown in the diagram below from Western Digital, when the Sentinel ECC&DSP error correcting system detects a low error rate, a lower gear utilizing less power is applied—Gear 1. "However, as the [bit error rate] goes up, [Gear 1] fails at some point to decode with high probability. At that point, the higher resolution gear kicks in."[10] On information and belief, this means the Accused Products utilize an error correction architecture that monitors the bit-error rate for the different flash cells in the products and selectively powers up additional error correction coding based on the number of errors present.[11]

---

[7] *See The Application of ECC/DSP to Flash Memory*, available online at https://documents.westerndigital.com/content/dam/doc-library/en_us/assets/public/western-digital/collateral/white-paper/white-paper-the-application-of-ecc-dsp-to-flash-memory.pdf (last visited Sept. 15, 2021).

[8] *See id.* at 5-6.

[9] *See id*.

[10] *See id*.

[11] *See id*.

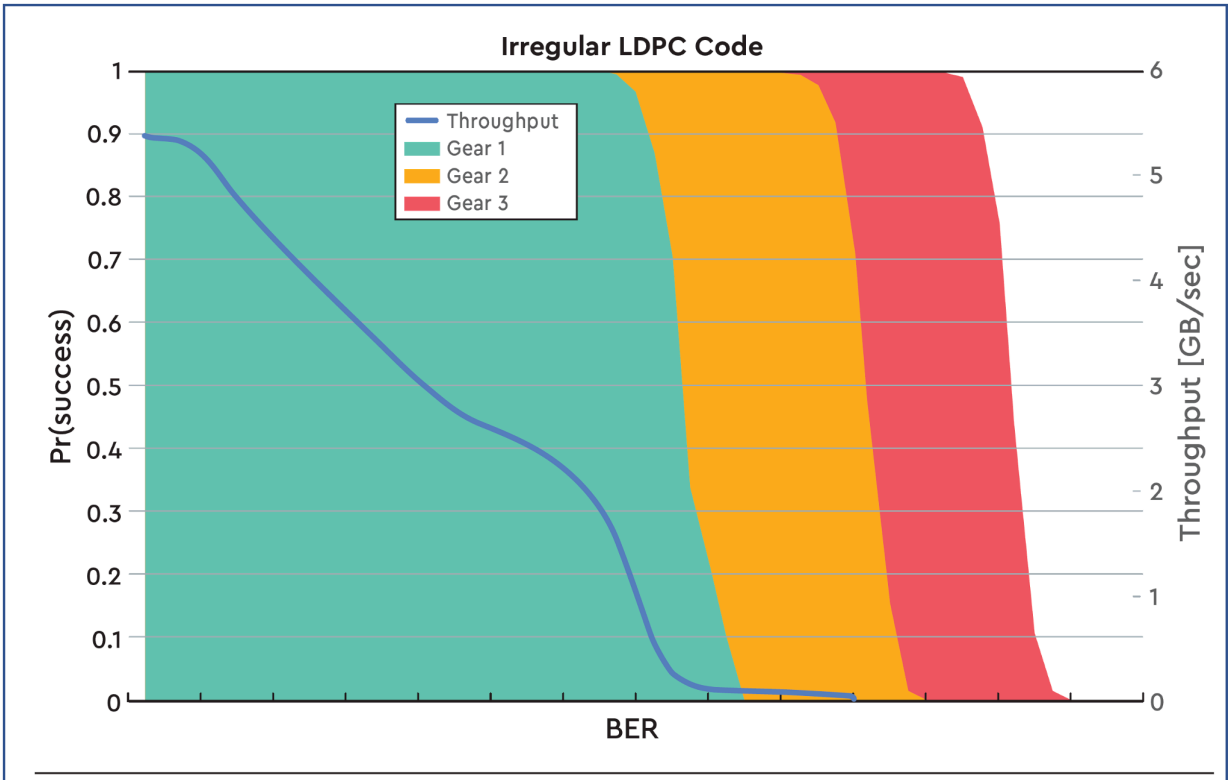


Figure 5: Example of various decoding gears correction capability and overall performance

50. Moreover, to maintain adequate speed with its devices, Western Digital's Sentinel ECC&DSP error correcting system processes error detection and correction in a parallel and physically separate process through its multiple "gears." As Western Digital describes it, "the ECC engine in gears 1, 2, 3 is segregated in a manner that it can serve separate requests in separate gears simultaneously."[12] On information and belief, therefore, the Accused Products utilize a parallel architecture for processing data through its error detection and correction system and the detection and correction portions of that system are physically separate from each other.

51. Viasat's patented FEC architecture improves the overall reliability and lifespan of the Accused Products' flash devices, both of which are, on information and belief, key drivers of sales of the Accused Products. According to Western Digital:

[12] *See id.* at 7.

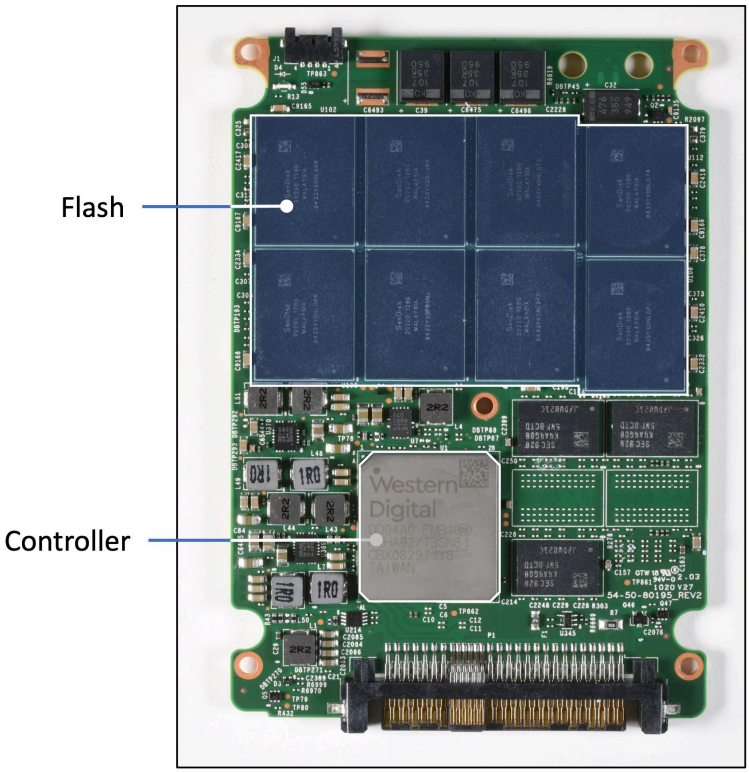
> "Implementing an ECC mechanism improves the overall reliability of the flash device, as read, write and data retention errors are caught and corrected. Less known is the fact that a strong ECC engine is one of the most important factors to increase the life span of a flash device. When blocks start to age, more and more errors will occur on that block. When the ECC engine is not able to correct these errors, a hard 'ECC' error occurs and the block will be retired. The more powerful the ECC engine, the more 'life' can be squeezed out of a [memory] block (even though it shows increasing failures) and the longer the overall lifespan of the flash device."[13]

52. In addition, the monitoring and adaptive error correction in the '347 patent extend the life and improve the performance of the Accused Products. The benefits to the Accused Products from the '347 patent's claimed method or architecture results in lower power consumption, better performance, and higher endurance for the Accused Products. These factors are, on information and belief, drivers of sales of the Accused Products.

53. One example of an infringing SSD is Western Digital's WDS960G1D0D SN600 SSD, such as the unit depicted below.

[13] *See Western Digital, White Paper: Flash 101 and Flash Management* at 13-14 (Aug. 2018), available online at https://documents.westerndigital.com/content/dam/doc-library/en_us/assets/public/western-digital/collateral/white-paper/white-paper-sandisk-flash101-management.pdf.

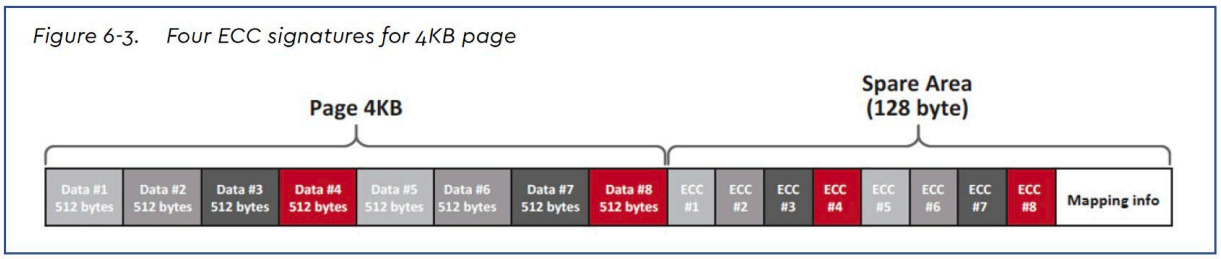
54. Western Digital's WDS960G1D0D SN600 SSD contains multiple flash-memory packages and a Western Digital flash memory controller or third-party controller adapted for use within Western Digital products.[14] On information and belief, all versions of the WDS960G1D0D SN600 SSD utilize the Sentinel ECC&DSP error correcting system.



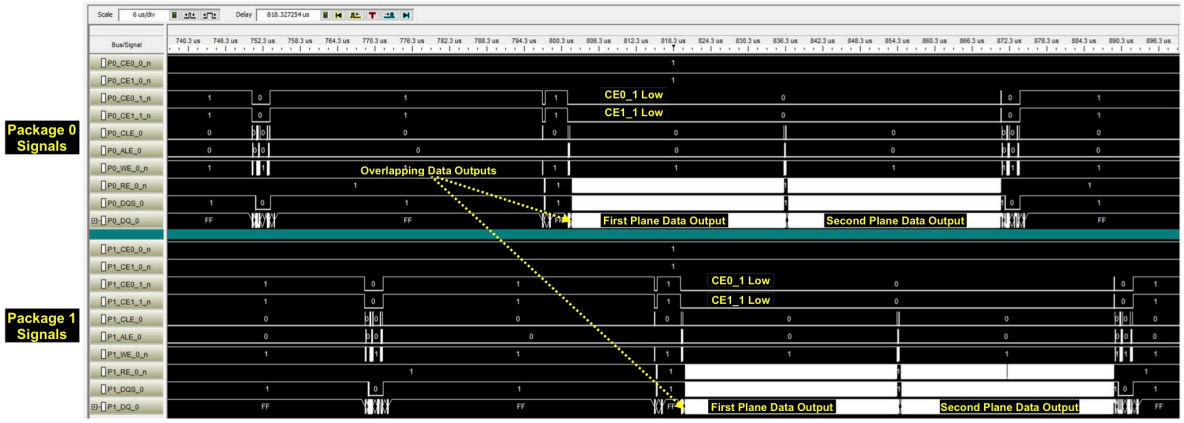
55. On information and belief, the controller in the WDS960G1D0D SSD includes a flash memory decoder and a decoding module configured to receive data with an ECC signature, such as that displayed below, taken from a Western Digital White Paper publication regarding its flash memory products, for a 4KB page flash with 8 ECC signatures (one for each 512 bytes of

[14] *See Western Digital Introduces WD Gold Enterprise SSDs*, available online at https://www.anandtech.com/show/15577/western-digital-introduces-wd-gold-enterprise-ssds (last visited Sept. 15, 2021).

data).[15]



56. On information and belief, the decoder in the WDS960G1D0D SSD generates a plurality of partially decoded data streams from the encoded data it receives from the flash memory. Notably, when a stream containing multiple packages of data is sent through the decoder, the decoder splits the data into discrete packages, as demonstrated by the simultaneous real time "overlapping" data output of Package 0 and Package 1 Signals below.



57. On information and belief, the flash memory controller in the WDS960G1D0D SSD further contains an error detection module that is communicatively coupled with the decoder and comprises a number of sub-modules operating in parallel. Each error detection sub-module can receive a partially decoded data stream, detect whether a portion of the respective

[15] *See Western Digital, White Paper: Flash 101 and Flash Management*, available online at https://documents.westerndigital.com/content/dam/doc-library/en_us/assets/public/western-digital/collateral/white-paper/white-paper-sandisk-flash101-management.pdf.

stream contains an error, and forward on the portion of the stream that contains an error to an error correction module.

58. Notably, in a "White Paper" published by Western Digital on the application of ECC to flash memory, Western Digital describes "Error Detection" and "Error Correction" as separate mechanisms effectuated by their own unique algorithms. According to this literature, error detection occurs "[e]very time a page of data" is retrieved from the flash memory. An ECC signature is created based on the "read-back data" and compared to the ECC signature that was created when the data was first stored to determine if any errors are present.[16]

59. On information and belief, the error correction modules in the Accused Products are physically separate from the error detection modules and configured to correct the received portions of the respective data streams containing an error. Again according to Western Digital's own White Papers, error correction occurs only "if the two [ECC] signatures differ," *i.e.*, if an error has been detected, after which the relevant data is forwarded on and corrected before being provided to the user.[17]

CLAIM I: INFRINGEMENT OF U.S. PATENT NO. 8,615,700

60. Viasat incorporates by reference and re-alleges the foregoing paragraphs of this Complaint.

61. Western Digital has infringed and continues to infringe at least claim 1 of the '700 patent by making, using, selling, offering for sale, and importing the Accused Products without authority or license in violation of 35 U.S.C. § 271(a).

[16] *See id.* at 13.

[17] *Id*.

62. The Accused Products infringe at least claim 1 of the ’700 patent. Representative claim 1 recites the following error-correction system:

> 1. A flash memory decoder comprising:
>
> a decoding module configured to:
>
> receive encoded data from the flash memory; and
>
> decode the received encoded data to generate a plurality of partially decoded data streams;
>
> an error detection module communicatively coupled with the decoding module, and comprising a plurality of error detection sub-modules operating in parallel, each error detection sub-module configured to:
>
> receive a different one of the plurality of partially decoded data streams;
>
> detect whether a portion of the respective received stream contains an error; and
>
> forward the portion of the respective received stream containing an error to an error correction module; and
>
> the error correction module, communicatively coupled with and physically separate from the error detection module, and configured to correct the received portions of the respective received streams containing an error.

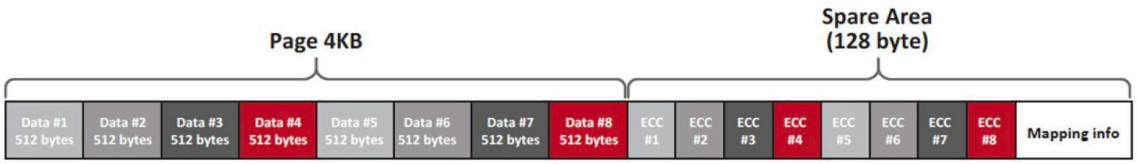
63. The Accused Products all contain flash memory and a controller (including a flash memory decoder). By way of non-limiting example, on information and belief, Western Digital’s WDS960G1D0D SN600 SSD (“WDS960G1D0D SSD”) meets each and every limitation of claim 1 of the ’700 patent. Western Digital’s WDS960G1D0D SN600 SSD contains multiple flash-memory packages and a Western Digital controller.[18]

64. The Accused Products all contain a flash memory decoder comprising a decoding module configured to receive encoded data from flash memory. For example, on information and

[18] *See Western Digital Introduces WD Gold Enterprise SSDs*, available online at https://www.anandtech.com/show/15577/western-digital-introduces-wd-gold-enterprise-ssds.

belief, the controller in the WDS960G1D0D SSD includes a flash memory decoder comprising a decoding module configured to receive data with ECC encoding. As Western Digital disclosed in a White Paper publication regarding its flash memory products, the Accused Products, including the WDS960G1D0D SSD, utilize standard ECC protocols that encode an ECC signature along with the stored data, as shown below.[19]

Figure 6-3. Four ECC signatures for 4KB page



65. On information and belief, as part of the read-out of data from the flash memory, the encoded data (in the form of the stored data and ECC signature) is received by the decoding module, as described below in Western Digital's White Paper.[20]

6.3 Error Detection and Correction

The maximum number of errors that can be detected and corrected is determined by the algorithm. No matter what algorithm is used within the ECC engine of a NAND flash controller, the method of error detection and correction remains the same:

* * *

3. When reading the data back, both data and stored ECC signature are read into the controller. A new ECC signature is generated, based upon the read-back data.

[19] *See Western Digital, White Paper: Flash 101 and Flash Management* at 14, available online at https://documents.westerndigital.com/content/dam/doc-library/en_us/assets/public/western-digital/collateral/white-paper/white-paper-sandisk-flash101-management.pdf.

[20] *See id.* at 13.

66. The Accused Products' decoding modules are also configured to decode the received encoded data to generate a plurality of partially decoded data streams. For example, on information and belief, the controller in the WDS960G1D0D SSD includes a flash memory decoder comprising a decoding module configured to receive encoded data from flash memory and then decodes the received encoded data to generate a plurality of partially decoded data streams. Communication between the flash and the controller occurs over a channel of control and data signals. Each channel goes to a separate NAND flash die. The controller receives streams of ECC encoded data from multiple channels of flash in parallel, which is partially decoded. Multiple independent channels of data are received, each with its own ECC encoding that are to be decoded in chunks as the parallel streams come into the controller. The controller decodes the received encoded data by generating a new ECC signature based on the read-back data. This process is described below, from a Western Digital White Paper.[21]

> **6.3 Error Detection and Correction**
>
> The maximum number of errors that can be detected and corrected is determined by the algorithm. No matter what algorithm is used within the ECC engine of a NAND flash controller, the method of error detection and correction remains the same:
>
> * * *
>
> 3. When reading the data back, both data and stored ECC signature are read into the controller. A new ECC signature is generated, based upon the read-back data.

67. Similarly, on information and belief Western Digital's proprietary Sentinel ECC&DSP error correcting system, contained in all of its NAND-flash-memory-containing products, decodes the received encoded data to generate a plurality of partially decoded data

[21] *Id.*

streams in order to facilitate the parallel and simultaneous detection and correction of data errors through its ECC engine gears.[22]

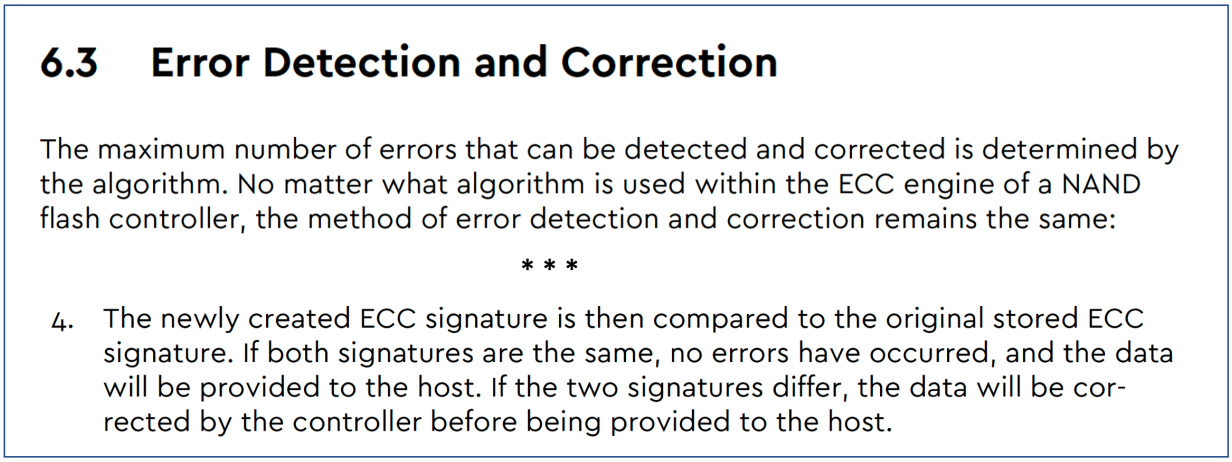
68. The Accused Products' flash memory decoder also comprises an error detection module communicatively coupled with the decoding module. For example, the controller in the WDS960G1D0D SSD includes an error detection module communicatively coupled with the decoding module that receives the partially decoded data streams from the decoding module. On information and belief, data is sent from flash memory through to the controller, which contains an error detection module that receives partially decoded data streams. Similarly, on information and belief Western Digital's proprietary Sentinel ECC&DSP error correcting system, contained in all of its NAND-flash-memory-containing products, contains an error detection module communicatively coupled with the decoding module that receives the partially decoded data streams from the decoding module as evidenced by its ability to detect the severity of the bit error rate and appropriately select the ECC engine "gear" for error correction.[23]

69. On information and belief, the Accused Products' error detection modules also comprise a plurality of error detection sub-modules operating in parallel, each error detection sub-module configured to receive a different one of the plurality of partially decoded data streams, detect whether a portion of the respective received stream contains an error, and forward the portion of the respective received stream containing an error to an error correction module. For example, on information and belief, the controller in the WDS960G1D0D SSD contains an error detection module comprising a plurality of error detection sub-modules operating in

[22] *See The Application of ECC/DSP to Flash Memory* at 7, available online at https://documents.westerndigital.com/content/dam/doc-library/en_us/assets/public/western-digital/collateral/white-paper/white-paper-the-application-of-ecc-dsp-to-flash-memory.pdf.

[23] *Id.* at 5-7.

parallel, each error detection sub-module configured to: receive a different one of the plurality of partially decoded data streams, detect whether a portion of the respective received stream contains an error, and forward the portion of the respective received stream containing an error to an error correction module. The stream of data with partially decoded ECC encoding is decoded in chunks as parallel streams come into the error detection module. The error detection module compares the original stored ECC signature to the newly generated ECC signature. Any detected error is forwarded to the error correction module.[24]



6.3 Error Detection and Correction

The maximum number of errors that can be detected and corrected is determined by the algorithm. No matter what algorithm is used within the ECC engine of a NAND flash controller, the method of error detection and correction remains the same:

* * *

4. The newly created ECC signature is then compared to the original stored ECC signature. If both signatures are the same, no errors have occurred, and the data will be provided to the host. If the two signatures differ, the data will be corrected by the controller before being provided to the host.

70. Similarly, on information and belief Western Digital's proprietary Sentinel ECC&DSP error correcting system, contained in all of its NAND-flash-memory-containing products, processes error detection and correction in a parallel and physically separate process through its multiple "gears." As Western Digital describes it, "the ECC engine in gears 1, 2, 3 is segregated in a manner that it can serve separate requests in separate gears simultaneously."[25] On

[24] *See Western Digital, White Paper: Flash 101 and Flash Management* at 13, available online at https://documents.westerndigital.com/content/dam/doc-library/en_us/assets/public/western-digital/collateral/white-paper/white-paper-sandisk-flash101-management.pdf.

[25] *See The Application of ECC/DSP to Flash Memory* at 7, available online at https://documents.westerndigital.com/content/dam/doc-library/en_us/assets/public/western-digital/collateral/white-paper/white-paper-the-application-of-ecc-dsp-to-flash-memory.pdf.

information and belief, this describes how the Accused Products' error detection module comprises a plurality of error detection sub-modules operating in parallel, each error detection sub-module configured to: receive a different one of the plurality of partially decoded data streams, detect whether a portion of the respective received stream contains an error, and forward the portion of the respective received stream containing an error to an error correction module.

71. On information and belief, the Accused Products' flash memory decoders also comprise an error correction module, communicatively coupled with and physically separate from the error detection module, and configured to correct the received portions of the respective received streams containing an error. For example, on information and belief, the controller in the WDS960G1D0D SSD has an error correction module, communicatively coupled with and physically separate from the error detection module and configured to correct the received portions of the respective received streams containing an error. On information and belief, the Accused Products implement modules in a hardware implementation physically separate from the error detection modules to evaluate error location and correct errors. Moreover, Western Digital describes how its proprietary Sentinel ECC&DSP error correcting system, contained in all of its NAND-flash-memory-containing products, maintain adequate speed with its devices by processing error detection and correction in a parallel and physically separate process through its multiple "gears." As Western Digital describes it, "the ECC engine in gears 1, 2, 3 is segregated in a manner that it can serve separate requests in separate gears simultaneously."[26] On information and belief, therefore, the Accused Products utilize a parallel architecture in which the error correction module, communicatively coupled with and physically separate from the

[26] *Id.*

error detection module, is configured to correct the received portions of the respective received streams containing an error.

CLAIM TWO: INFRINGEMENT OF U.S. PATENT NO. 8,966,347

72. Viasat incorporates by reference and re-alleges the foregoing paragraphs of this Complaint.

73. Western Digital has infringed and continues to infringe at least claim 1 of the '347 patent by making, using, selling, offering for sale, and importing the Accused Products without authority or license in violation of 35 U.S.C. § 271(a).

74. The Accused Products meet the limitations of at least claim 1 of the '347 patent. Representative claim 1 recites the following method:

> 1. A method comprising:
>
> encoding data using forward error correction coding;
>
> storing the encoded data in a flash memory;
>
> retrieving the encoded data stored in the flash memory to generate a data stream;
>
> processing, using at least a first error correction sub-module, the data stream to correct errors in the data stream associated with the flash memory;
>
> monitoring a metric of the flash memory while repeating the encoding, the storing, the retrieving and the processing, wherein the metric represents memory performance degradation of the flash memory;
>
> determining that the monitored metric exceeds a threshold;
>
> in response to the determination, modifying the forward error correction coding for use in subsequently encoding data for storage in the flash memory; and
>
> in response to the determination, powering-up, from an inactive mode, a second error correction sub-module arranged in parallel with the first error correction sub-module for subsequent data stream processing.

75. The Accused Products all practice a method comprising encoding data using forward error correction coding. On information and belief, Western Digital's proprietary Sentinel ECC&DSP error correcting system, contained in all of its NAND-flash-memory-containing products, uses a method of error correction comprising encoding data based on the forward error correction coding known as Low Density Parity Check coding. [27]

> The Sentinel ECC&DSP error correction is based on state-of-the-art Low Density Parity Check (LDPC) coding and provides a full suite of NAND DSP (Digital Signal Processing) services, including data randomization or shaping, NAND health metering via Bit Error Rate (BER) estimation, ECC-based read thresholds calibration, and NAND defect protection and recovery via XOR based RAID scheme support.

76. The Accused Products all practice a method comprising storing the encoded data in flash memory and retrieving the encoded data stored in the flash memory to generate a data stream. As depicted below, data is encoded and stored in NAND flash dies and subsequently retrieved from the flash as a data stream.[28]

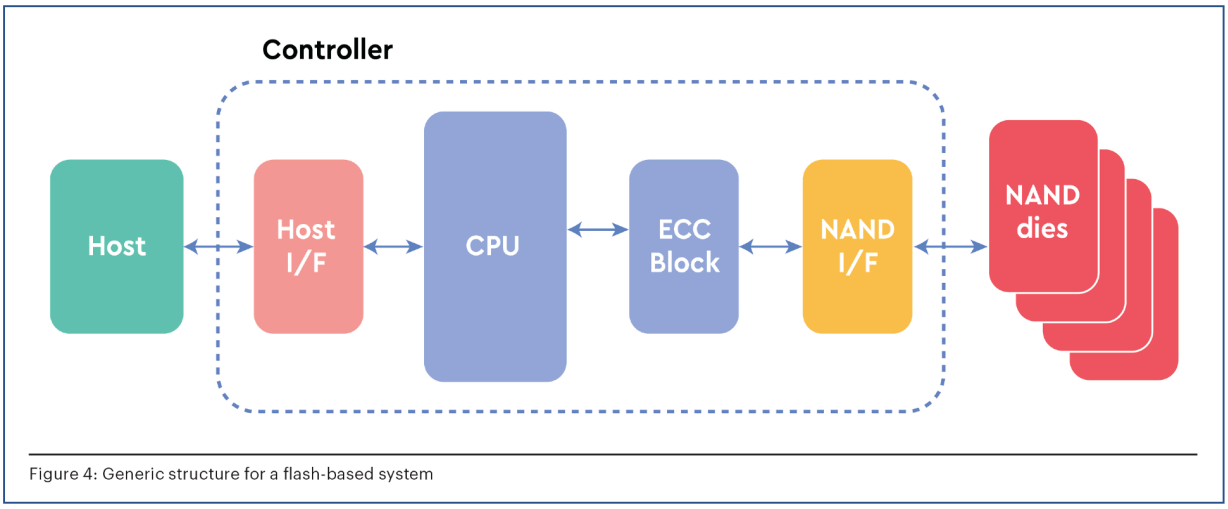


Figure 4: Generic structure for a flash-based system

[27] *Id.* at 5-7.

[28] *Id.*

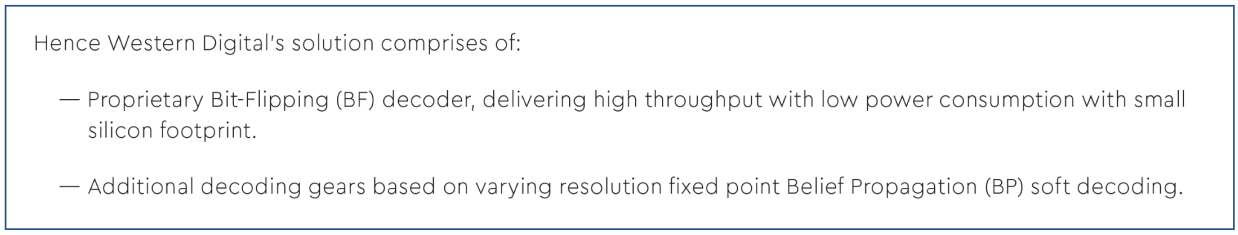
77. Similarly, Western Digital's description of how its error correction system works states that it stores the encoded data in the flash memory and retrieves the encoded data to generate a data stream read back into the controller.[29]

> **6.3 Error Detection and Correction**
>
> The maximum number of errors that can be detected and corrected is determined by the algorithm. No matter what algorithm is used within the ECC engine of a NAND flash controller, the method of error detection and correction remains the same:
>
> * * *
>
> 3. When reading the data back, both data and stored ECC signature are read into the controller. A new ECC signature is generated, based upon the read-back data.

78. The Accused Products all practice a method comprising processing, using at least a first error correction sub-module, the data stream to correct errors in the data stream associated with the flash memory. On information and belief, Western Digital's proprietary Sentinel ECC&DSP error correcting system, contained in all of its NAND-flash-memory-containing products, processes the data stream with at least the first error correction sub-module of its Bit-Flipping decoder to correct errors in a low bit-rate-error environment, delivering high throughput with low power consumption.[30]

[29] *See Western Digital, White Paper: Flash 101 and Flash Management* at 13, available online at https://documents.westerndigital.com/content/dam/doc-library/en_us/assets/public/western-digital/collateral/white-paper/white-paper-sandisk-flash101-management.pdf.

[30] *See The Application of ECC/DSP to Flash Memory* at 6, available online at https://documents.westerndigital.com/content/dam/doc-library/en_us/assets/public/western-digital/collateral/white-paper/white-paper-the-application-of-ecc-dsp-to-flash-memory.pdf.


Hence Western Digital's solution comprises of:

— Proprietary Bit-Flipping (BF) decoder, delivering high throughput with low power consumption with small silicon footprint.

— Additional decoding gears based on varying resolution fixed point Belief Propagation (BP) soft decoding.

79. The Accused Products all practice a method comprising monitoring a metric of the flash memory while repeating the encoding, the storing, the retrieving and the processing, wherein the metric represents memory performance degradation of the flash memory. For example, the Sentinel ECC&DSP error correcting system has what Western Digital describes as a "multi-gear architecture." The Sentinel ECC&DSP error correcting system monitors at least the bit-error rate for the flash memory (a metric representing at least in part memory performance degradation of the flash memory) and selects a higher or lower power "gear" for the error correcting system depending on the severity of the bit-error rate—as can be seen in the figure below. [31]

[31] *Id.* at 5-6.

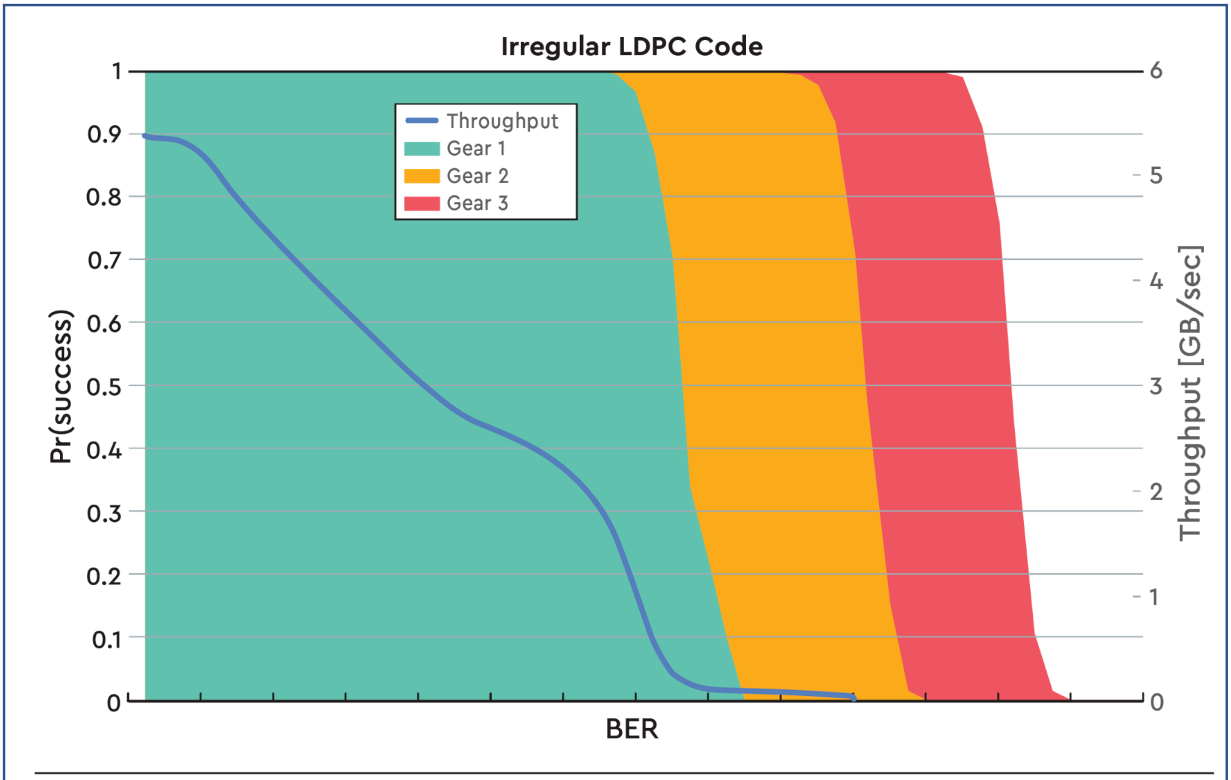


Figure 5: Example of various decoding gears correction capability and overall performance

80. The Accused Products all practice a method comprising determining that the monitored metric exceeds a threshold; in response to the determination, modifying the forward error correction coding for use in subsequently encoding data for storage in the flash memory; and in response to the determination, powering-up, from an inactive mode, a second error correction sub-module arranged in parallel with the first error correction sub-module for subsequent data stream processing. On information and belief, the Accused Products modify the forward error correction coding for use in subsequently encoding data for storage in the flash memory by, for example, adapting the code rate or shutting down sectors of the flash memory that exceed the predefined bit-error rate.[32]

[32] *Id.* at 11.

> **Puncturing and Shortening.** As the ECC decoder is set to operate in high throughput the common layered approach is employed. This approach mandates to use layer granularity during encoding and decoding operations as to process simultaneously large number of bits. In order to maintain high resolution of information and parity shortening and puncturing operations are supported in both encoder and decoder modules. This feature is set to accommodate full usage of the available NAND cells in the physical page while enabling flexibility in code rate for numerous applications / scenarios.

81. Moreover, on information and belief, these additional "gears" are utilized in parallel and only powered up from inactivity when needed to maximize efficiency of power use. As Western Digital describes it, in order to maintain adequate speed with its devices, "the ECC engine in gears 1, 2, 3 is segregated in a manner that it can serve separate requests in separate gears simultaneously."[33] On information and belief, therefore, the Accused Products, in response to the determination that the flash memory performance has degraded in excess of a threshold, power-up, from an inactive mode, a second error correction sub-module arranged in parallel with the first error correction sub-module for subsequent data stream processing.

82. The Accused Products all practice a method comprising, in response to the determination, powering-up, from an inactive mode, a second error correction sub-module arranged in parallel with the first error correction sub-module for subsequent data stream processing.[34]

> When the BER is high, there is no point in spending decoder time trying to decode with lower gears, as this would only degrade performance by adding unnecessary latency to the decoding sequence. Consequently, the LDPC engine estimates the BER of the noisy page as part of its initialization process by counting the number of unsatisfied parity checks. This forms the basis on which it automatically chooses the appropriate decoding gear.
>
> Furthermore, the parallelism of each decoding gear is dimensioned according to its usage probability (given the memory BER distribution) and the overall required decoding throughput. Thus, the number of costly high-resolution processing units instantiated for the full resolution BP decoder, which is rarely used ("safety net"), could be much lower than the number of simple BF processing units. This approach significantly reduces the ASIC footprint with a negligible impact on overall sustained decoding throughput.

[33] *Id.* at 7.
[34] *Id.* at 6-7.

DEMAND FOR A JURY TRIAL

83. Viasat requests a trial by jury of all issues so triable under Fed. R. Civ. P. 38.

PRAYER FOR RELIEF

WHEREFORE, Viasat respectfully requests that the Court:

A. Enter judgment in favor of Viasat that Western Digital has infringed one or more claims of the '700 and/or '347 patents, directly and indirectly, literally or under the doctrine of equivalents;

B. Award damages sufficient to compensate Viasat for Western Digital's infringement under 35 U.S.C. § 284;

C. Find this case exceptional under 35 U.S.C. § 285 and award Viasat its reasonable attorneys' fees;

D. Award Viasat costs and expenses associated with maintaining this action;

E. Award pre-judgment and post-judgment interest; and

F. Provide any other relief that the Court deems appropriate.

Dated: November 29, 2021

Respectfully submitted,

/s/ Melissa R. Smith

Melissa R. Smith
State Bar No. 24001351
GILLAM & SMITH, LLP
303 South Washington Avenue
Marshall, Texas 75670
Telephone: (903) 934-8450
Facsimile: (903) 934-9257
Email: melissa@gillamsmithlaw.com

J. Scott McBride (*Pro Hac Vice* pending)
Matthew R. Ford (*Pro Hac Vice* pending)
Nevin M. Gewertz (*Pro Hac Vice* pending)

BARTLIT BECK LLP
54 W. Hubbard Street, Suite 300
Chicago, IL 60654
(312) 494-4400
scott.mcbride@bartlitbeck.com
matthew.ford@bartlitbeck.com
nevin.gewertz@bartlitbeck.com

Nosson D. Knobloch (*Pro Hac Vice* pending)
BARTLIT BECK LLP
1801 Wewatta Street, Suite 1200
Denver, CO 80202
(303) 592-3100
nosson.knobloch@bartlitbeck.com

Counsel for Plaintiff